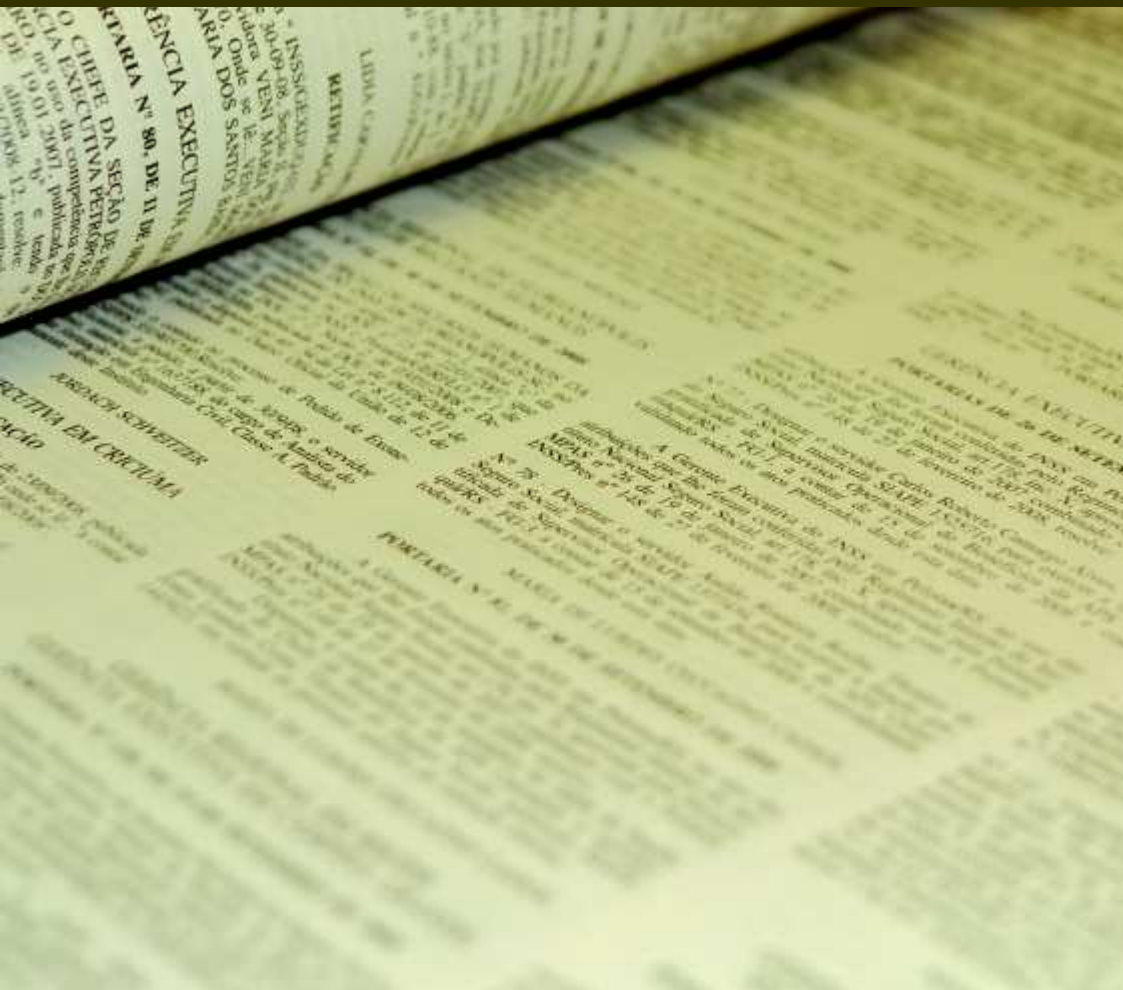
TRIBUNAL DE CONTAS DA UNIÃO

Sumários Executivos

Auditoria nos Sistemas de Informação do Diário Oficial da União



República Federativa do Brasil

Tribunal de Contas da União

Ministros

Ubiratan Aguiar, Presidente
Benjamin Zymler, Vice-Presidente
Valmir Campelo
Walton Rodrigues
Augusto Nardes
Aroldo Cedraz
Raimundo Carreiro
José Jorge
José Múcio

Auditores

Augusto Sherman
Marcos Bemquerer
André Luís de Carvalho
Weder de Oliveira

Ministério Público

Lucas Rocha Furtado, Procurador-Geral
Paulo Soares Bugarin, Subprocurador-Geral
Maria Alzira Ferreira, Subprocuradora-Geral
Marinus Eduardo de Vries Marsico, Procurador
Cristina Machado da Costa e Silva, Procuradora
Júlio Marcelo de Oliveira, Procurador
Sérgio Ricardo Costa Caribé, Procurador

Negócio
Controle Externo da Administração Pública
e da gestão dos recursos públicos federais

Missão
Assegurar a efetiva e regular gestão dos
recursos públicos em benefício da sociedade

Visão
Ser instituição de excelência no controle e contribuir
para o aperfeiçoamento da Administração Pública

TRIBUNAL DE CONTAS DA UNIÃO

Sumários Executivos

Auditoria nos Sistemas de Informação do Diário Oficial da União

Relator
Ministro Raimundo Carreiro

Brasília, 2010

Brasil. Tribunal de Contas da União.
Auditoria nos Sistemas de Informação do Diário Oficial da União / Relator Raimundo Carreiro. – Brasília : TCU, 2010.
36 p. – (Sumários Executivos)

1. Publicação oficial - auditoria. 2. Segurança de dados. I. Diário Oficial da União. II. Título.

Catalogação na fonte: Biblioteca Ministro Ruben Rosa

SUMÁRIO

APRESENTAÇÃO

Os sumários executivos da Secretaria de Fiscalização de Tecnologia da Informação (Sefti) do Tribunal de Contas da União têm por objetivo divulgar os principais resultados das fiscalizações de Tecnologia da Informação (TI) realizadas pela Sefti. As publicações contêm, de forma resumida, aspectos importantes verificados durante as auditorias, recomendações e determinações para melhorar a governança de TI na Administração Pública Federal e, também, boas práticas identificadas.

O foco das fiscalizações de Tecnologia da Informação realizadas pela Sefti é a verificação da conformidade e do desempenho das ações governamentais nessa área, a partir de análises sistemáticas de informações sobre aspectos de governança, segurança e aquisições de bens e serviços de TI, utilizando critérios fundamentados. O principal objetivo dessas fiscalizações é contribuir para o aperfeiçoamento da gestão pública, para assegurar que a tecnologia da informação agregue valor à atuação da Administração Pública Federal em benefício da sociedade.

Pretende-se com a divulgação desses trabalhos, oferecer aos parlamentares, aos órgãos governamentais, à sociedade civil e às organizações não-governamentais informações suficientes e fidedignas para que possam exercer o controle das ações de governo.

Este número traz as principais informações sobre a auditoria realizada nos sistemas de informação que suportam o Diário Oficial da União, de responsabilidade da Imprensa Nacional, órgão subordinado à Casa Civil da Presidência da República. O respectivo processo (TC nº 023.616/2008-0) foi apreciado em Sessão Extraordinária de Caráter Reservado do Plenário do TCU, de 13 de maio de 2009, sob a relatoria do Ministro Raimundo Carreiro.

Ubiratan Aguiar
Ministro-Presidente

RESUMO

A presente auditoria teve como objetivo verificar a situação da segurança da informação nos sistemas da Imprensa Nacional (IN), órgão subordinado à Casa Civil da Presidência da República, em especial nos sistemas que suportam o Diário Oficial da União (DOU), tendo em vista a relevância desse instrumento para a sociedade brasileira. Os trabalhos foram realizados durante o período de 1º de setembro a 31 de outubro de 2008.

Foram identificados, como principais achados de auditoria, inexistência de Política de Segurança da Informação, de Política de Controle de Acesso e de Plano de Continuidade do Negócio. Também foram evidenciadas falhas na gestão da segurança da informação e no processo de geração do DOU. Além disso, foram encontradas impropriedades em contratos de serviços de terceirização de Tecnologia da Informação (TI), entre as quais destaca-se o pagamento de valores a maior, cujo ressarcimento aos cofres públicos estava sendo providenciado pelo órgão.

As propostas de encaminhamento englobam determinações e recomendações para estabelecimento de políticas e de mecanismos para melhorar a gestão da segurança das informações da Imprensa Nacional, assim como para a conformidade dos processos de contratação.

Os benefícios estimados das determinações e recomendações são melhorias na forma de atuação, no planejamento e na gestão da segurança da informação na Imprensa Nacional, nos controles internos, na segurança dos sistemas e recursos informatizados, na qualidade das informações geradas pelos sistemas, além de redução de custos administrativos. Estima-se ainda uma economia no valor de R$ 283.197,27 (duzentos e oitenta e três mil, cento e noventa e sete reais e vinte e sete centavos), referente à glosa de pagamentos efetuados a maior e regularização da contabilização mensal dos serviços prestados em um dos contratos fiscalizados.

O DIÁRIO OFICIAL DA UNIÃO

O Diário Oficial da União (DOU) é o veículo de comunicação oficial pelo qual são tornados públicos os atos dos três poderes da União, bem como os atos de estados e municípios cuja publicidade seja condição necessária para assegurar a validade e produção regular de seus efeitos. Para produzir o DOU, a Imprensa Nacional (IN) utiliza-se de sistemas de informação que atuam desde o recebimento das matérias encaminhadas para publicação até a editoração do jornal. Esse processo informatizado finaliza com a geração de um arquivo eletrônico a ser utilizado na impressão do DOU e no sistema de consulta dos jornais disponibilizado no sítio da IN.

Os atos oficiais a serem publicados no DOU são encaminhados por meio do sistema de envio e recebimento eletrônico de matérias (INCom). Esse sistema tem por finalidade a transmissão dos atos oficiais mediante rotinas automatizadas de geração de ofício eletrônico, compactação de dados, recebimento e transferência de matérias para publicação no DOU, conforme estabelecido no art. 33 da Portaria nº 310/2002 da Imprensa Nacional, que dispõe sobre as normas técnicas para publicação de atos nos Diários Oficiais.

O sistema INCom possui dois módulos: um utilizado pelos usuários externos para encaminhamento das matérias, denominado INCom Web; e outro utilizado pelos usuários internos da IN para gerenciamento desse recebimento, chamado INCom View. Esses módulos também permitem o acompanhamento da situação da matéria quanto à publicação, por meio da atribuição de estados que informam se a matéria ainda não foi tratada (aguardando), se foi liberada para publicação (liberada) ou se foi rejeitada (devolvida).

Para utilizar o INCom, os órgãos e entidades das três esferas da Federação, bem como outras pessoas jurídicas interessadas em integrar o sistema, devem formalizar pedido de cadastramento de um gerente por meio de ofício assinado por autoridade competente. Esse gerente pode cadastrar novos

gerentes ou usuários comuns para utilizarem o INCom. Para encaminharem as matérias para publicação, esses usuários recebem um certificado digital individual, gerado pela Imprensa Nacional, que visa garantir a autenticidade e integridade dos arquivos enviados.

Por questões de ordem técnica que resultem na impossibilidade da utilização do INCom, é possível entregar mídia magnética com as matérias a serem publicadas diretamente à Gerência de Recebimento, Seleção e Registro de Matérias (Gerem) da IN, ou enviá-la pelo correio, acompanhada de ofício assinado discriminando as matérias encaminhadas para publicação. Mesmo nessas situações, as matérias são incluídas no INCom pelo servidor da Gerem que as recebeu. Em suma, todas as matérias publicadas no DOU passam necessariamente por esse sistema.

Para serem publicadas na data prevista, as matérias devem ser encaminhadas à IN até as 18 horas do dia útil anterior ao previsto para publicação. As matérias enviadas após esse horário serão publicadas automaticamente no dia útil subsequente, conforme regra estabelecida no sistema INCom, em consonância com a Portaria nº 310/2002 da IN.

Para cancelar a publicação de uma matéria, o cliente deve encaminhar solicitação por meio de ofício, fax ou correio eletrônico, não sendo possível comandar o cancelamento por intermédio do sistema INCom.

Após serem recebidas pelo sistema INCom, as matérias que preenchem os requisitos de data e horário para publicação no dia útil subsequente são disponibilizadas para a fase de editoração do jornal, e têm o estado atualizado para liberada. Essa fase é realizada com o apoio do software *GoodNews* (GN3).

A primeira etapa de editoração do jornal consiste na revisão das matérias encaminhadas, tendo em vista a verificação da conformidade com as regras de publicação, bem como a correção de erros de forma que não interfiram no

seu conteúdo. As matérias desconformes são devolvidas ao órgão/entidade e têm seu estado atualizado no sistema INCom para devolvida.

A etapa seguinte, chamada de retranca, consiste em unir as matérias em arquivos que originarão as páginas do jornal na etapa de paginação. Esta é a última etapa de editoração do jornal.

Em todas essas etapas pode ocorrer a desativação da matéria, em decorrência de algum outro problema que não tenha sido considerado na Portaria em questão, mas, ainda assim, justificaria sua não publicação. Entretanto, essa desativação não é refletida, como estado da matéria, no sistema INCom.

Uma vez finalizada a paginação, é gerado o arquivo do DOU em formato *postscript*[1] (extensão ".ps") para impressão na área gráfica. O mesmo arquivo também dá origem à edição eletrônica disponibilizada para acesso gratuito, por intermédio do título "Pesquisa" no portal da IN, bem como para assinantes, via sistema e-Diários.

A pesquisa de jornal, disponibilizada no portal da Imprensa Nacional, permite consultar tanto a versão completa do DOU quanto as páginas individuais do jornal que atendam aos critérios de busca pré-definidos. O sistema e-Diários, por sua vez, acessado mediante pagamento de assinatura, disponibiliza para cópia (*download*) as edições completas dos jornais até o 3º dia útil subsequente à sua publicação, nos termos estabelecidos na Portaria nº 282/2008 da Imprensa Nacional.

O QUE FOI AVALIADO PELO TCU

Foram avaliados os sistemas de informação e os recursos de TI da Imprensa Nacional, em especial os envolvidos no processo de produção e publicação do Diário Oficial da União, sob a ótica da segurança da informação. Buscou-se identificar falhas que comprometeriam a segurança das informações processadas pelo órgão, tendo em vista a preservação da

integridade, confidencialidade, autenticidade e disponibilidade dessas informações. Além disso, avaliou-se a conformidade das contratações de serviços de terceirização de TI.

Para avaliar a gestão da segurança da informação, foram elaboradas questões de auditoria que abordaram a verificação da existência de análise de risco, políticas de segurança da informação, de controle de acesso, de *backup* e de continuidade do negócio, levando em consideração a conformidade com a legislação pertinente e boas práticas recomendadas pelas normas técnicas utilizadas.

Em relação aos sistemas que suportam a geração do DOU, a questão elaborada buscou verificar se as bases de dados dos sistemas eram consistentes, no sentido de garantir a integridade e o respeito às regras de negócio definidas na legislação.

No que tange aos contratos de serviços de terceirização de TI, a questão definida teve a intenção de verificar se os respectivos processos de contratação estavam de acordo com a legislação pertinente e entendimentos do TCU. O volume de recursos fiscalizados foi de R$ 10.507.579,89 (dez milhões, quinhentos e sete mil, quinhentos e setenta e nove reais e oitenta e nove centavos), que corresponde à soma dos valores dos contratos de prestação dos seguintes serviços:

- Serviços técnicos especializados em Tecnologia da Informação (TI), complementares às atividades da Imprensa Nacional, nas áreas de Administração e Operação de Rede, Administração de Banco de Dados, Manutenção de Sistemas e Suporte Técnico;
- Serviços complementares de Tecnologia da Informação e de Comunicação de dados à Imprensa Nacional para:
    - Disponibilização e integração da Imprensa Nacional aos sistemas corporativos e à Infovia do Governo federal;
    - Consultoria em soluções de segurança e de certificação digital;

- Fornecimento de soluções em software livre;
- Implantação de contingência dos serviços da Imprensa Nacional;
- Implantação de recursos de multimídia e acessibilidade;
- Recuperação, conversão para meios digitais e organização de acervos documentais;
- Integração de correios eletrônicos;
- Capacitação e treinamento;
- Consultoria e apoio à gestão de TI.

- Serviços especializados para suporte, manutenção evolutiva e corretiva da solução integrada da Contratante de envio, recebimento e editoração de matérias e produção eletrônica dos jornais oficiais (INJOR). A solução integrada INJOR é composta pelo sistema INCom e pelas funções customizadas pela Imprensa Nacional do software *GoodNews* (GN3).

POR QUE FOI AVALIADO

Esta auditoria foi aprovada pelo Plenário deste Tribunal, a partir de proposta formulada pelo ministro Raimundo Carreiro na sessão reservada de 18 de junho de 2008. O trabalho teve como objetivo verificar a situação da segurança da informação nos sistemas da IN, em especial nos sistemas que suportam o Diário Oficial da União, tendo em vista a relevância desse instrumento para a sociedade brasileira. A escolha por uma auditoria com a abordagem de segurança da informação foi motivada pela situação identificada na Imprensa Nacional a partir do Levantamento de Governança de Tecnologia da Informação da Administração Pública Federal, realizado pela Sefti no ano de 2007 (TC 008.380/2007-1, Acórdão nº 1.603/2008 – TCU – Plenário). Na oportunidade, verificou-se a ausência de políticas e normas que poderiam comprometer o adequado tratamento das informações por parte daquele órgão.

COMO SE DESENVOLVEU O TRABALHO

Durante o planejamento da auditoria, a equipe coletou informações sobre a Imprensa Nacional na internet, em trabalhos realizados pelo Tribunal, e em documentos, normas e manuais solicitados à IN referentes aos recursos de TI envolvidos no processo de geração do Diário Oficial da União. Também foi realizada uma reunião com a diretoria da Imprensa Nacional para apresentação dos sistemas que suportam o DOU e da infraestrutura de TI do órgão.

O planejamento da auditoria foi elaborado tendo como referência a Lei n.º 8.666/1993, os Decretos nºs 2.271/1997, 3.505/2000, 4.520/2002, 4.521/2002 e 4.553/2002, a Instrução Normativa GSI nº 1/2008, os princípios constantes da Constituição Federal de 1988 aplicáveis à Administração Pública, normativos do próprio órgão e, principalmente, controles previstos nas normas da Associação Brasileira de Normas Técnicas (ABNT) que tratam de práticas para a gestão da segurança da informação, NBR ISO/IEC 27002:2005 (Gestão da Segurança da Informação) e NBR ISO/IEC 27005:2008 (Gestão de Riscos da Segurança da Informação).

A despeito do objeto desta auditoria ser a segurança da informação nos sistemas da Imprensa Nacional, fez parte do escopo do trabalho a análise da conformidade dos processos de contratação de serviços de TI, em especial acerca dos entendimentos proferidos pelo TCU. Essa abordagem foi motivada por recente diretriz da Sefti de incluir, de forma sistêmica, em suas auditorias, a verificação dos contratos de TI, em maior ou menor profundidade, conforme o objeto da auditoria. De forma a não comprometer o foco central do trabalho, restringiu-se essa verificação aos seguintes tópicos dos contratos específicos de terceirização na área de TI:

- Modalidade de licitação adotada;
- Modelo de gestão do contrato;
- Estimativa de preço;

- Medição utilizada para fins de pagamento;
- Cláusulas que garantam a segurança das informações.

Na execução da auditoria, dentre outros procedimentos, foram realizadas entrevistas com coordenadores e gerentes, tanto das áreas de negócios quanto do setor de TI, e funcionários terceirizados das atividades de TI, tendo como intuito obter informações que permitissem avaliar aspectos específicos da segurança da informação no órgão e a gestão e execução dos contratos de TI. No trabalho, realizou-se adicionalmente o exame documental dos normativos e procedimentos documentados pelo órgão, assim como dos processos licitatórios fiscalizados.

A equipe de auditoria solicitou a extração dos dados do sistema de recebimento de matérias (INCom), correspondente ao período de 2004 a 2008, com o objetivo de verificar, utilizando-se de ferramentas de análise automática de dados, a consistência entre o conteúdo enviado e o publicado. Para isso, seria necessário extrair também a base de dados do software de editoração eletrônica, *GoodNews*. Contudo, em face do reduzido tempo de guarda dos dados dos jornais gerados, não foi solicitada a referida extração, o que restou por comprometer a automatização e o escopo da verificação pretendida.

Dessa forma, a consistência entre o enviado e o publicado foi avaliada a partir de uma amostra de 60 matérias de uma determinada prefeitura, por meio de comparação entre o conteúdo dos arquivos recebidos pelo sistema INCom com as respectivas publicações impressa e eletrônica do DOU.

O QUE O TCU ENCONTROU

Gestão de segurança da informação

Falhas na análise de risco

Diante do elevado custo da gestão da segurança da informação em uma organização, é recomendável que ela seja guiada pelos riscos específicos do negócio, identificados, quantificados e priorizados quando da realização da análise de riscos, cujos resultados constituem instrumentos para a orientação, determinação e implementação dos controles selecionados e priorizados, de maneira a proteger a organização contra esses riscos, de acordo com a NBR ISO/IEC 27002:2005, item 4 – Análise/avaliação e tratamento de riscos.

A norma NBR ISO/IEC 27005:2008, específica para gestão de riscos de segurança da informação, nos itens 6 e 9, traz como parte do processo de gestão de riscos a implementação de um plano de tratamento do risco que, com base na lista de riscos aos quais está sujeita a organização, ordenados por prioridade, define as ações e os controles necessários para reduzir os riscos a um nível aceitável, com os seus prazos de execução e custos associados.

Acerca da análise de riscos da Imprensa Nacional, três aspectos devem ser considerados. Primeiro o de que não se evidenciou que o Plano Diretor de Segurança da Informação (PDSI) apresentado tenha sido ratificado pelo órgão, na medida em que não há responsabilidades, prioridades e cronograma específico definidos, nem documento da alta direção firmando compromisso com o plano, embora a IN tenha ponderado que o PDSI tenha sido aprovado em reunião de coordenadores com a Direção-Geral. Assim, o plano figura como sugestão do Serpro para a Imprensa Nacional, sem a certeza da realização dos projetos ali contidos, não podendo, portanto, ser considerado como Plano Diretor de Segurança da Informação da Imprensa Nacional.

O segundo diz respeito ao planejamento das ações e controles que deveriam ser implementados pela IN para mitigação dos riscos identificados. Iniciativas estão sendo realizadas por parte da Coordenação de Tecnologia da Informação, sem que tenha havido, contudo, a priorização das ações e dos controles, a designação dos respectivos responsáveis e o estabelecimento dos prazos.

Por fim, o terceiro aspecto refere-se à necessidade da realização periódica da análise de riscos. Recomenda-se a realização de nova análise sempre que ocorrerem mudanças na estrutura de TI do órgão.

Falhas na Política de Segurança da Informação

De acordo com o item 2.3 da cartilha Boas Práticas em Segurança da Informação do TCU, Política de Segurança da Informação é:

> Um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela organização para que sejam assegurados seus recursos computacionais e suas informações.

A Instrução Normativa GSI nº 1, de 13 de junho de 2008, em seu art. 5º, inciso VII, atribui aos órgãos da APF sob sua jurisdição competência para aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações, de sua competência.

Essa orientação vai ao encontro das boas práticas preconizadas pela NBR ISO/IEC 27002:2005, que, em seu item 5.1 – Política de Segurança da Informação, recomenda que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização.

Foram solicitadas informações à Imprensa Nacional acerca da Política de Segurança da Informação (PSI) existente no órgão. Os gestores apresentaram uma minuta de política de uso de recursos de TI em fase final de análise, para posterior submissão à Direção-Geral para aprovação e implantação.

A minuta apresentada seria uma norma complementar à PSI, não podendo ser considerada como a própria, em razão dos seguintes aspectos:

- Falta de declaração de comprometimento da alta direção;
- Política restrita à TI;
- Não aborda classificação da informação;
- Não versa sobre tratamento de riscos;
- Não define responsabilidades para a gestão da segurança da informação, incluindo tratamento de incidentes;
- Trata de aspectos operacionais e não sobre princípios e diretrizes.

Embora não possua uma PSI já instituída no órgão, o Plano Diretor de Tecnologia da Informação da Imprensa Nacional (PDTI/IN), para o período de 2008-2010, aprovado pela Portaria nº 141/2008, estabelece como diretriz relativa à gestão da segurança da informação: "desenvolver, implementar e praticar uma política institucional de segurança da informação, definida a partir de análises de risco e de investimento". Contudo, faz-se necessário o comprometimento da alta direção com a questão, visto que a necessidade da elaboração da norma foi exposta em abril de 2007, quando da elaboração do Plano Diretor de Segurança da Informação pelo Serpro, e até o momento o órgão não possui política formalizada.

Falhas na gestão da segurança da informação

A norma NBR ISO/IEC 27002:2005 recomenda que uma estrutura de gerenciamento da segurança da informação seja estabelecida na or-

ganização. No item 6.1.2 – Coordenação da segurança da informação, a norma recomenda que as atividades de segurança da informação sejam coordenadas por representantes de áreas relevantes da organização para garantir a conformidade com a política de segurança da informação. No item 6.1.3 – Atribuição de responsabilidades para a segurança da informação, a norma recomenda que todas as responsabilidades pela proteção dos ativos de informação estejam claramente definidas.

Com relação à gestão de incidentes de segurança da informação, a NBR ISO/IEC 27002:2005 recomenda, no item 13.1 – Notificação de fragilidades e eventos de segurança da informação, que sejam estabelecidos procedimentos formais para que fragilidades e eventos de segurança da informação sejam comunicados tempestivamente por meio de canais apropriados. No item 13.2 – Gestão de incidentes de segurança da informação e melhorias, a norma recomenda que responsabilidades e procedimentos sejam estabelecidos para assegurar respostas efetivas a incidentes de segurança da informação e que as informações de incidentes ocorridos sejam utilizadas para melhoria contínua da gestão desses incidentes.

A Instrução Normativa GSI nº 1/2008 aprovou orientações para a gestão de segurança da informação e comunicações que deverão ser implementadas pelos órgãos e entidades da Administração Pública Federal (art. 1º), definindo competências para, dentre outras, nomear Gestor de Segurança da Informação e Comunicações (art. 5º, inciso IV), instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais (art. 5º, inciso V) e instituir Comitê de Segurança da Informação e Comunicações (art. 5º, inciso VI).

Na Imprensa Nacional, a situação encontrada foi inexistência de gestor de segurança da informação com competência para coordenar ações em toda a organização, inexistência de normativo definindo as responsabilidades para a segurança da informação, inexistência de comitê de segurança para assessorar a implementação das ações relacionadas e inexistência de equipe

com responsabilidade de tratar e responder a incidentes de segurança na rede de computadores.

Observou-se durante a auditoria que as ações de segurança da Impressa Nacional estão restritas à operacionalização da tecnologia da informação e que não há participação de outras áreas relevantes da organização. Observaram-se também deficiências nos controles internos e procedimentos não padronizados conforme relatado nos demais achados.

Inexistência de Política de Controle de Acesso

A norma NBR ISO/IEC 27002:2005, no item 11.1.1 – Política de Controle de Acesso, recomenda que as regras de controle de acesso e direitos para cada usuário ou grupo de usuários sejam expressas claramente em uma política de controle de acesso.

A Portaria nº 147/2006 da Casa Civil da Presidência da República, Regimento Interno da Imprensa Nacional, no art. 15, incisos X e XI, estabelece que a Coordenação de Tecnologia da Informação (Corti) tem competência para definir e implementar padrões e critérios de segurança de acesso, guarda, recuperação e comunicação de dados, bem como gerenciar o acesso de usuários internos e externos aos sistemas, aplicativos e demais serviços relacionados com a tecnologia da informação.

A Imprensa Nacional apresentou uma minuta de política de acesso e procedimentos que disciplinava o controle de acesso (lógico e físico) a recursos computacionais e sistemas de informação, que, segundo o órgão, estava em fase final de análise, com vistas a posterior submissão à Direção-Geral para aprovação e implantação. Não existia, portanto, uma política de controle de acesso formalmente definida e aprovada.

No que se refere à minuta de política apresentada, verificou-se uma série de deficiências que comprometem a eficácia do resultado pretendido:

- É incompleta, pois é restrita ao acesso à rede (senha de acesso) e à internet, não contemplando os demais recursos;
- Não leva em consideração os requisitos de segurança dos sistemas de informação da Imprensa Nacional;
- Não estabelece e nem faz referência a regras de controle de acesso e direitos (perfis) para os usuários dos sistemas;
- Não é baseada em classificação das informações;
- Não é baseada nos riscos a que as informações estão expostas;
- Não estabelece segregação de funções para controle de acesso: pedido, autorização e administração;
- Não estabelece procedimento para autorização formal de pedidos de acesso;
- Não estabelece processo formal para análise crítica periódica de acessos.

A ausência de política de controle de acesso formalmente estabelecida contribui para a existência de procedimentos não padronizados e deficiência nos controles de acesso aos sistemas e aplicações, podendo trazer dificuldade de responsabilização, e risco de ocorrência de acessos não autorizados e de vazamento de informações.

Falhas no gerenciamento de usuários

Verificou-se que os processos relativos ao gerenciamento de usuário, os quais contemplam o registro de usuário, o gerenciamento de privilégios, o gerenciamento de senhas e a análise crítica dos direitos de acesso, não estavam devidamente formalizados, conforme recomendações constantes dos itens 11.2.1, 11.2.2, 11.2.3 e 11.2.4 da NBR ISO/IEC 27002:2005. Não obstante, avaliou-se a efetividade dos procedimentos existentes para controlar o acesso aos recursos de TI que apóiam e operacionalizam a geração do DOU.

A diretriz constante da alínea *a* do item 11.2.1 da norma em tela recomenda que as contas de usuário (identificadores de usuário) sejam únicas para assegurar a responsabilidade de cada usuário por suas ações e que o compartilhamento de contas somente deve ser utilizado quando existir necessidade para o negócio ou por razões operacionais, devidamente aprovadas e documentadas. Nesse caso, é essencial que as atividades realizadas por esses tipos de conta sejam devidamente registradas, conforme preconiza o item 10.10.4 da referida norma.

Verificou-se, por meio de observação direta nos sistemas e entrevistas com integrantes da Corti, a existência de contas de usuários compartilhadas no âmbito daquela coordenação. Uma dessas contas é utilizada para disponibilização do DOU no portal da Imprensa Nacional.

Apurou-se ainda que contas dos sistemas de gerenciamento de banco de dados são compartilhadas pelos técnicos terceirizados responsáveis pelo serviço. Além disso, identificou-se conta compartilhada pelos usuários da Coordenação de Editoração e Divulgação Eletrônica dos Jornais Oficiais (Coejo).

Registre-se que não foi apresentado à equipe de auditoria qualquer documento justificando a necessidade da existência desses compartilhamentos, bem como se verificou, por meio de entrevistas e verificação *in loco*, que as atividades realizadas por essas contas não são registradas.

O item 11.2.4 da NBR ISO/IEC 27002:2005 recomenda que o gestor "conduza a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal". Entre as orientações sugeridas para a realização desse processo, destaca-se a revisão desses direitos "depois de qualquer mudança, como promoção, rebaixamento ou encerramento do contrato" do usuário.

Foi informado pela Corti que esse tipo de análise é feito com periodicidade mensal. Contudo, foram identificados usuários que se desligaram do

órgão e permaneceram com as respectivas contas ativas. De uma amostra de catorze usuários com conta no GN3 ou INcom View, dez não possuíam mais vínculo com a IN. Desses dez usuários desligados, dois permaneciam com contas ativas (habilitadas), dois estavam com contas inativas (desabilitadas) e seis não foram localizados (provavelmente excluídos) no serviço de diretório da rede.

Evidencia-se, portanto, além da falha na remoção dos direitos de acesso dos usuários que deixam o órgão, a falta de padronização quando esse procedimento é executado, uma vez que há usuários que são excluídos e outros apenas desabilitados nos sistemas.

Observou-se ainda, quando do cadastramento de usuário interno nos sistemas da IN, que não é passada uma declaração por escrito com os direitos de acesso respectivos, e, por via de consequência, não é solicitada a assinatura do usuário indicando seu entendimento acerca das condições de acesso, situações que também contrariam diretrizes estabelecidas no item 11.2.1 da referida norma.

Por fim, foram identificados usuários com perfil de acesso não condizente com a função desempenhada.

Falhas na política e uso de senha

Não existem procedimentos implementados, tanto no INCom Web quanto no serviço de diretório da rede de computadores da IN, que obriguem o usuário a escolher senhas de qualidade (por exemplo, exigir quantidade mínima de caracteres e não permitir senhas com todos os caracteres repetidos), bem como modificar regularmente sua senha, conforme preconiza o item 11.3.1 da NBR ISO/IEC 27002:2005.

Falhas na política de *backup*

A norma NBR ISO/IEC 27002:2005, no item 10.5 – Cópias de segurança, recomenda que procedimentos de rotina sejam estabelecidos para implementar cópias de segurança (*backup*s), incluindo a geração das cópias e testes de recuperação. No item 15.1.3 – Proteção de registros organizacionais, a norma recomenda que "os procedimentos de armazenamento e manuseio sejam implementados de acordo com as recomendações de fabricantes" devido à possibilidade de deterioração das mídias e que, para mídias eletrônicas, "sejam incluídos procedimentos para assegurar a capacidade de acesso aos dados (leitura tanto na mídia quanto no formato utilizado) durante o período de retenção, para proteger contra perdas ocasionadas pelas futuras mudanças na tecnologia".

A documentação referente à política de *backup* da IN não define procedimentos regulares para teste de recuperação dos dados armazenados nas mídias, tampouco foi aprovada formalmente pelo órgão (NBR ISO/IEC 27002:2005, item 10.5.1, diretrizes f e g).

De fato, observou-se que não são realizados testes regulares das informações contidas nas fitas, para verificar a completude dos dados e a integridade das mídias. Isso ficou evidenciado quando a Corti não conseguiu extrair alguns dados relacionados com a publicação de matérias do DOU, que estariam gravados em fitas antigas do tipo DLT (*Digital Linear Tape*).

Outra falha identificada diz respeito à localização do cofre, onde estão guardadas as fitas de *backup*, que não está de acordo com as orientações contidas na NBR ISO/IEC 27002:2005.

Inexistência de Plano de Continuidade do Negócio (PCN)

A NBR ISO/IEC 27002:2005, no item 14.1, enuncia que o objetivo de um PCN é não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, as-

segurar sua retomada em tempo hábil, se for o caso, e manter a integridade e a disponibilidade dos dados e serviços da organização.

A situação encontrada é de inexistência de um plano de continuidade do negócio para a Imprensa Nacional, embora conste do Plano Diretor da Segurança da Informação (PDSI), a sugestão para a elaboração de um modelo de gestão da continuidade do negócio e de um PCN. O Plano Diretor de Tecnologia da Informação (PDTI), para o período de 2008-2010, aprovado pela Portaria nº 141/2008, também estabelece, como diretriz relativa à gestão da tecnologia, a adoção e manutenção de amplo e consistente plano de continuidade que garanta a atuação da Imprensa Nacional.

Sistemas que suportam o DOU

Inconsistência no sistema INCom

O sistema INCom é responsável pelo recebimento das matérias a serem publicadas no DOU. Esse sistema, entre outras funcionalidades, informa o estado das matérias encaminhadas para publicação. O estado de liberada, para uma matéria com data de publicação anterior à atual, a princípio, indica que a matéria foi publicada. Por exemplo, uma matéria enviada até às 18h do dia 9/10/2008, para publicação no dia 10/10/2008, exibida como liberada no INCom, deveria ter sido publicada nesta data. Caso o envio tenha ocorrido após o horário precitado, deveria ser publicada no dia útil subsequente, conforme depreende-se do art. 30 da Portaria nº 310/2002 da Imprensa Nacional.

Verificou-se, todavia, que o sistema INCom pode apresentar como liberadas matérias cuja publicação no DOU não se realizou. Essa situação foi evidenciada documentalmente pela equipe de auditoria.

Além disso, cabe registrar a insuficiência de registros de operações que possibilitem monitorar todo o ciclo de vida das matérias, do recebimento à publicação, uma vez que nem todas as alterações sofridas pelas matérias na

fase de editoração eletrônica são refletidas no sistema INCom. Esses registros são recomendados no item 10.10.1 da NBR ISO/IEC 27002:2005.

Falha no processo de cancelamento de matéria

A Portaria nº 310/2002 da Imprensa Nacional, estabelece, no art. 18, que o pedido de cancelamento das matérias deve ser encaminhado à Coordenação de Editoração e Divulgação Eletrônica (Coejo) por meio de ofício, fax, correio eletrônico ou diretamente pelo sistema de envio eletrônico (INCom), contendo, entre outros, a assinatura do responsável pelo cancelamento.

Ressalte-se que a portaria não especifica o tipo de assinatura que deve ser utilizada no correio eletrônico e no sistema de envio eletrônico de matérias. Todavia, tendo em vista que o objetivo do dispositivo é garantir a autenticidade e a integridade do pedido de cancelamento, a assinatura digital seria o mecanismo adequado para conferir segurança a esse procedimento.

Acerca da segurança nas comunicações eletrônicas, o item 10.8.4 da NBR ISO/IEC 27002:2005 recomenda que as informações que trafegam em mensagens eletrônicas sejam adequadamente protegidas, e sugere, nas diretrizes para implementação, que as considerações de segurança da informação sobre essas mensagens incluam, entre outros itens, aspectos legais, como, por exemplo, assinatura digital.

Contudo verificou-se, por observação direta, que o cancelamento de matérias, solicitado por meio de correio eletrônico, não utiliza de meios eficazes para assegurar a autenticidade e integridade da mensagem de solicitação encaminhada.

Descumprimento do procedimento de envio de matérias

O Decreto nº 4.520 e a Portaria nº 310 da Imprensa Nacional, ambos de 2002, estabelecem, nos arts. 11 e 24, respectivamente, que o recebimento de

matérias para publicação no Diário Oficial da União e no Diário da Justiça deve ser realizado exclusivamente por meio de transmissão eletrônica.

A Portaria, ao dispor as normas para a publicação de matérias nos Diários Oficiais, institui um sistema próprio ao envio eletrônico de matérias, o sistema INCom, e impõe, como requisito para a transmissão eletrônica, o efetivo cadastramento do emitente nesse sistema. Em seu art. 27, o normativo permite a intermediação por empresas privadas, conhecidas por agências intermediadoras, para efeito de transmissão de atos pelo sistema INCom, mediante procuração do órgão/entidade emitente.

Tendo em conta a possibilidade de ocorrência de problemas de ordem técnica que eventualmente possam vir a impedir o envio de matérias por meio eletrônico, a Portaria autoriza a entrega de matérias diretamente nas dependências da Imprensa Nacional.

Dessa forma, pelo normativo, o recebimento de matérias em mídia magnética na IN deve ser eventual. Verificou-se, contudo, a prática rotineira dessa forma de envio de matérias, principalmente das matérias encaminhadas com intermediação de empresas privadas. O problema dessa permissividade, além da desconformidade com o normativo vigente, é, sob o olhar da segurança da informação, a inclusão de terceiros em um processo que deveria relacionar somente o emitente com o sistema INCom, o que facilita a ocorrência de erros e fraudes.

Segundo informações obtidas nas entrevistas realizadas com os gestores da IN, os órgãos/entidades que contratam as empresas privadas são, em sua maioria, prefeituras e secretarias estaduais. Eles o fazem não só para terceirizar todo o processo de envio de matérias, mas também, na maioria das vezes, por desconhecerem o sistema eletrônico provido e a facilidade do processo implementado pela IN, ou mesmo a possibilidade do envio de matérias sem intervenção de empresa. Ainda segundo relato dos gestores, as empresas cobram uma taxa do órgão/entidade por essa intermediação. Embora o valor cobrado não esteja submetido ao exame da IN, já houve

informação de taxa cobrada no percentual de 400% sobre o custo de publicação da matéria.

Ausência de certificação digital dos diários oficiais

O Decreto nº 4.520/2002, que dispõe sobre a publicação do Diário Oficial da União e do Diário da Justiça pela Imprensa Nacional, em seu §2º do art. 1º, estabelece que:

As edições eletrônicas do Diário Oficial da União e do Diário da Justiça, disponibilizadas no sítio da Imprensa Nacional e necessariamente certificadas digitalmente por autoridade certificadora integrante da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, produzem os mesmos efeitos que as em papel.

O art. 3º do Decreto nº 4.521/2002, emitido na mesma data, ao dispor sobre a autonomia administrativa, financeira e técnica da Imprensa Nacional, ressalta a necessidade de certificação dos jornais: "o acesso aos atos oficiais disponibilizados no sítio da Imprensa Nacional, necessariamente certificados digitalmente por autoridade certificadora da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, é gratuito".

Verificou-se, todavia, que, embora as edições eletrônicas do Diário Oficial da União disponibilizadas no Portal da IN na internet sejam acessadas por meio de certificação digital do sítio e, portanto, por meio de uma conexão segura na qual as informações trafegam de forma criptografada, elas próprias não são assinadas ou certificadas digitalmente.

A certificação digital de um sítio assegura sua autenticidade[2] e, por meio da confidencialidade[3] da comunicação (conexão segura) entre as partes, a integridade[4] do documento em relação à transferência pela internet. Ou seja, essa certificação busca impedir a leitura ou alteração das informações enquanto estas são enviadas. Entretanto, essa certificação não é suficiente para assegurar a autenticidade e integridade dos documentos eletrônicos

disponibilizados, pois não garante que o documento original (idêntico ao impresso) não tenha sido modificado na origem.

Identificou-se ainda, mediante acesso ao sistema e-Diários, que as edições eletrônicas do DOU, disponibilizadas exclusivamente para assinantes, também não estão assinadas digitalmente.

Falhas no monitoramento de atividades dos usuários

Com o objetivo de detectar atividades não autorizadas, a norma NBR ISO/IEC 27002:2005, no item 10.10 – Monitoramento, recomenda que o uso de sistemas de informação e recursos de TI seja monitorado por meio de registros cronológicos de atividades (logs) e trilhas de auditoria.

Durante as entrevistas realizadas com os gestores da Corti e verificações feitas nos sistemas da Imprensa Nacional que operacionalizam o DOU, foram encontradas algumas falhas relacionadas ao monitoramento das atividades realizadas pelos usuários internos.

Identificou-se a inexistência de registros das atividades (*logs*) dos usuários administradores do serviço de diretório da rede de computadores da IN e dos servidores de bancos de dados.

Verificou-se, ainda, que os administradores de banco de dados podem realizar operações diretamente nas bases de dados com o uso de programas utilitários. Por necessidade de serviço, os administradores estão autorizados a realizar esse tipo de operação, mas não há autorização formal nem registros dos procedimentos realizados, conforme orientações contidas no item 11.5.4 da NBR ISO/IEC 27002:2005.

Foi constatada também a insuficiência de registros de atividades (*logs*) que possibilitem fornecer trilhas de auditoria para a base de dados dos sistemas da IN, o que impossibilita a realização de auditorias para averiguar problemas decorrentes de erros ou fraudes.

Embora, por questões de desempenho e espaço de armazenamento, não seja viável registrar todas as operações realizadas nas bases de dados, devem ser implementados controles que permitam rastrear atividades críticas e realizar futuras auditorias nos dados armazenados, seguindo as orientações constantes dos itens 10.10.1 e 10.10.2 da NBR ISO/IEC 27002:2005.

O mecanismo de sincronização de relógios não está implementado em todos os computadores e dispositivos de rede. É importante que os relógios estejam corretamente ajustados para evitar inconsistências de tempo que não permitam que matérias sejam publicadas em função do horário de seu recebimento. A sincronia dos relógios assegura a credibilidade dos registros de atividades dos usuários. Orientações nesse sentido encontram-se no item 10.10.6 da NBR ISO/IEC 27002:2005.

Contratos de terceirização de TI

Falhas no modelo de gestão do contrato

Para assegurar que o serviço entregue pela empresa contratada está de acordo com o especificado e atende às necessidades do órgão, é necessária a avaliação da qualidade do serviço. Esta deve ser aferida por meio de critérios objetivos (indicadores), de forma que a medição seja clara e transparente. Com a utilização desses critérios, é possível estabelecer escalas de valores e patamares mínimos de qualidade considerados aceitáveis, que, quando não atingidos, evitam que produto inadequado seja recebido e permitem a adoção de medidas saneadoras, bem como a aplicação de penalidades à contratada pelo descumprimento contratual.

Todos os contratos analisados não apresentam critérios de aceitação de serviços, não apresentam exigência de níveis de serviço nem discriminam mecanismos de controle sobre os requisitos exigidos e pontuados na proposta das empresas vencedoras. Dois dos contratos possuem cláusulas de penalidades genéricas, que, por não se reportarem a critérios objetivos de mensuração, são inaplicáveis.

Dessa forma, sem critérios de qualidade definidos e sem a discriminação mínima do que seria considerado descumprimento contratual, torna-se impraticável cobrar da contratada requisitos básicos dos serviços, como qualidade e prazo.

Observa-se ainda a opção indevida por postos de trabalho, na medida em que a medição e remuneração de todos os serviços abarcados por dois contratos são feitas com base na disponibilidade dos profissionais, não havendo vinculação aos resultados efetivamente atingidos, em ofensa ao art. 3º, §1º, do Decreto nº 2.271/1997.

Falhas na estimativa de preços

O processo originário de um dos contratos falha por não trazer a estimativa de preços nem o detalhamento dos custos no projeto básico ou na proposta apresentada pela empresa contratada. O valor estimado total para a prestação dos serviços é de 5 (cinco) milhões de reais, podendo chegar a 25 (vinte e cinco) milhões de reais, frente à possibilidade de sucessivas prorrogações. Contudo, não há, no processo, consultas ou pesquisas de preços, nem referência de como se chegou a esse valor.

Apesar de se tratar de contratação direta, a realização de estimativa de preço é etapa obrigatória no processo licitatório e sua ausência configura afronta à Lei nº 8.666/1993, art. 26, parágrafo único, inciso III.

Sem dúvida, a estimativa dos valores encontra um obstáculo diante da generalidade da descrição dos serviços a serem contratados, haja vista que os serviços são executados sob demanda, excluindo os serviços continuados, e somente no momento da solicitação ele é especificado e apreçado, o que contraria o art. 14 da Lei nº 8.666/1993.

Além disso, a contratação conjunta de serviços continuados e serviços não continuados gera a ocorrência de irregularidade quando da prorrogação contratual, pois os primeiros podem ter sua duração prorrogada por iguais e

sucessivos períodos, limitada a sessenta meses, enquanto que os outros não usufruem dessa prerrogativa, consoante o art. 57 da Lei nº 8.666/1993.

Falhas em cláusulas contratuais de segurança das informações

Nos termos dos arts. 59 e 60 do Decreto nº 4.553/2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, a celebração de contratos que envolvam o contato de pessoas com informações de natureza sigilosa deverá exigir dos interessados na contratação a assinatura de termo de compromisso de manutenção de sigilo e conter cláusulas prevendo a:

a) possibilidade de alteração do contrato para inclusão de cláusula de segurança não estipulada por ocasião da sua assinatura;

b) obrigação de o contratado manter o sigilo relativo ao objeto contratado, bem como à sua execução;

c) obrigação de o contratado adotar as medidas de segurança adequadas, no âmbito das atividades sob seu controle, para a manutenção do sigilo relativo ao objeto contratado;

d) identificação, para fins de concessão de credencial de segurança, das pessoas que, em nome do contratado, terão acesso a material, dados e informações sigilosos;

e) responsabilidade do contratado pela segurança do objeto subcontratado, no todo ou em parte.

A IN manipula informações de órgãos e entes da Administração Pública Federal que, em tese, são sigilosas até a respectiva publicação. Nesse sentido, faz-se necessário a proteção dessas informações quando tratadas tanto por servidores quanto por terceiros.

Constatou-se que dois contratos contêm cláusulas que impõem às contratadas a guarda do inteiro teor dos dados processados e o reconhecimento

de serem eles, bem como todo e qualquer sistema desenvolvido, incluindo sua documentação técnica, de propriedade exclusiva da contratante.

Entretanto, os citados contratos não contêm cláusulas que exijam dos contratados a assinatura do termo de compromisso de manutenção de sigilo, nem os requisitos a que se referem as alíneas *a, c, d* e *e* retro.

Existência de pagamentos a maior

Entre os diversos princípios que regem a licitação, dispostos no art. 3º da Lei nº 8.666/1993, encontra-se o princípio da vinculação ao instrumento convocatório, que impõe à Administração e ao licitante o dever de observarem as normas e condições estabelecidas no edital. Uma vez finalizada a licitação e firmado o contrato, a Administração e a contratada também estão vinculadas às cláusulas avençadas, segundo estabelecido no art. 66 da Lei nº 8.666/1993.

Em um dos contratos é especificado que o pagamento dos serviços seja realizado com base nas horas efetivamente trabalhadas, resultantes da multiplicação da quantidade de dias úteis do mês pelo número de horas correspondentes à jornada de trabalho, deduzindo-se ainda do resultado obtido, os afastamentos legais e/ou eventuais dos prestadores de serviço.

Dessa forma, resta configurada a hora de serviço prestado por cada profissional alocado como unidade básica para medição e pagamento dos serviços, sendo utilizadas ordens de serviço para solicitação dos serviços a serem executados.

Verificou-se nas ordens de serviço, onde constam as horas trabalhadas em cada mês por cada perfil profissional, que, em muitos meses, não havia variação nas horas computadas para os perfis profissionais. Ao se comparar o quantitativo das horas trabalhadas com o número de dias úteis de cada mês, verificou-se a cobrança de 22 dias de trabalho em meses com 20, 21 ou mesmo 23 dias úteis. Assim, as informações constantes das ordens de

serviço não refletem a realidade das horas trabalhadas e, por conseguinte, comprovam pagamentos indevidos à contratada.

Diante do fato, o Coordenador de Tecnologia da Imprensa Nacional, em anuência com o entendimento da equipe, orientou o fiscal do contrato a calcular os pagamentos realizados a maior desde o início da vigência do contrato (dezembro/2005) e a tomar as providências cabíveis para que se procedesse à glosa, nos próximos pagamentos, dos valores pagos indevidamente. Os cálculos efetuados pela IN apontam o total de R$ 169.918,36 (cento e sessenta e nove mil, novecentos e dezoito reais e trinta e seis centavos) a ser glosado.

Outros fatos relevantes

No decorrer da fase de execução da auditoria, a equipe deparou-se com fato não previsto nas questões de auditoria, mas que, em função de relevância e risco, mereceu atenção.

O fato diz respeito à recorrente queixa, por parte da Imprensa Nacional, quanto ao atual quadro permanente de pessoal da Coordenação de Tecnologia da Informação (Corti), considerado insuficiente para o cumprimento de suas competências, figurando como fator restritivo ao desenvolvimento de ações de governança e de segurança de TI.

Essa dificuldade foi apontada pelo gestor como uma das causas de diversos achados apontados no relatório. O Memorando nº 076 – Corti, de 15 de setembro de 2006, apresenta sugestão de contingente de pessoal por especificação, inclusive para os serviços terceirizados. Este documento, entretanto, não traz justificativas nem análises dos números sugeridos, que indicam necessidade de aumento de 500% no contingente, propondo mudança de 12 para 79 servidores.

Não obstante a falta de embasamento do dimensionamento da força de trabalho proposto para a Corti, é fato que a carência de pessoal no setor de

TI está presente, de forma geral, por toda a Administração Pública Federal, como reconhecido nos Acórdãos nos 140/2005, 2.023/2005, 786/2005 e 2.471/2008, todos do Plenário, havendo, neste último, recomendação à Secretaria-Executiva do Ministério do Planejamento, Orçamento e Gestão, com vistas à solução global do problema.

Em especial, a Imprensa Nacional, além de não possuir carreira específica de TI, não realiza concurso público há mais de 20 anos, sendo que muitos servidores estão próximos da aquisição do direito à aposentadoria.

O QUE PODE SER FEITO PARA MELHORAR A SEGURANÇA DA INFORMAÇÃO NA IMPRENSA NACIONAL

Com o objetivo de reduzir os riscos de segurança da informação inerentes às atividades da Imprensa Nacional, em especial os relacionados ao processo de produção do Diário Oficial da União, e de garantir a continuidade do negócio, foram expedidas determinações e recomendações ao órgão, entre as quais se destacam: implementação e formulação de uma política de segurança da informação; instituição de um comitê de segurança da informação; aprovação, formalização e disseminação de uma política de controle de acesso a informações e recursos de tecnologia da informação; correções de erros relacionados a procedimentos de controle de acesso; documentação e revisão dos procedimentos de *backup*; realização periódica de análise de risco; implementação de controles de segurança e correção de falhas nos sistemas que suportam o DOU.

Com relação às impropriedades verificadas nos contratos auditados, foram expedidas determinações para não prorrogação dos referidos instrumentos e regularização dos pagamentos a maior identificados em um dos contratos. Além disso, foram feitas determinações a serem observadas nas futuras contratações de TI, entre as quais se destacam: estabelecimento de critérios para aferição dos serviços prestados; detalhamento dos serviços licitados; elaboração de estimativa de preços e exigência de orçamentos detalhados dos serviços; parcelamento dos serviços face à natureza conti-

nuada ou não de sua execução; estabelecimento de cláusulas de segurança da informação nos contratos cujos prestadores de serviço manipulem informações de caráter sigiloso.

BENEFÍCIOS DA IMPLEMENTAÇÃO DAS DETERMINAÇÕES E RECOMENDAÇÕES DO TCU

Os benefícios estimados das determinações e recomendações são melhorias na forma de atuação, no planejamento e na gestão da segurança da informação na Imprensa Nacional, nos controles internos, na segurança dos sistemas e recursos informatizados, na qualidade das informações geradas pelos sistemas, além de redução de custos administrativos. Estima-se ainda uma economia no valor de R$ 283.197,27 (duzentos e oitenta e três mil, cento e noventa e sete reais e vinte e sete centavos), referente à glosa de pagamentos efetuados a maior e regularização da contabilização mensal dos serviços prestados em um dos contratos fiscalizados.

ACÓRDÃO Nº 1.033/2009 – TCU – PLENÁRIO

O acórdão que apreciou esta auditoria foi proferido em Sessão Extraordinária do Plenário, de Caráter Reservado, em 13 de maio de 2009, e consta na Ata nº 16/2009 – Plenário. Em virtude do caráter sigiloso da decisão, abstém-se de reproduzi-la nesta seção.

NOTAS

1 Linguagem formal para descrição gráfica precisa de documentos, que se tornou um padrão em editoração eletrônica (fonte: Dicionário Aurélio).

2 Autenticidade de informações consiste na garantia da veracidade da fonte das informações. Por meio da autenticação é possível confirmar a identidade da pessoa ou entidade que presta as informações (Cartilha de Boas Práticas de Segurança da Informação. 2a Ed. Tribunal de Contas da União, 2007).

3 Confidencialidade de informações consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento (Cartilha de Boas Práticas de Segurança da Informação. 2a Ed. Tribunal de Contas da União, 2007).

4 Integridade de informações consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados (Cartilha de Boas Práticas de Segurança da Informação. 2a Ed. Tribunal de Contas da União, 2007).

Responsabilidade pelo Conteúdo
Secretaria-Geral de Controle Externo:
Secretaria de Fiscalização de Tecnologia da Informação:

Equipe de Auditoria
Carlos Renato Araujo Braga (supervisor)
Mônica Cotrim Chaves (coordenadora)
Paulo Vinicius Silva de Castro
Sylvio Xavier Junior

Respondabilidade Editorial
Secretaria-Geral da Presidência
Instituto Serzedello Corrêa
Centro de Documentação
Editora do TCU

Capa e Diagramação
Paulo Brandão

Foto da capa
Paulo Brandão

Impresso pela Sesap/Segedam

TRIBUNAL DE CONTAS DA UNIÃO

Endereço para contato, solicitação de exemplares e consulta na Internet

TRIBUNAL DE CONTAS DA UNIÃO
Secretaria de Fiscalização de
Tecnologia da Informação (Sefti)
SAFS, Quadra 4, Lote 1
Anexo I, sala 311
70042-900 Brasília - DF
Fone: (61) 3316-5371/7396
Fax: (61) 3316-5372
http://www.tcu.gov.br/fiscalizacaoti
sefti@tcu.gov.br

Secretaria de Fiscalização de Tecnologia da Informação

Negócio

Controle externo da governança de tecnologia da informação na Administração Pública Federal.

Missão

Assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade.

Visão

Ser unidade de excelência no controle e no aperfeiçoamento da governança de tecnologia da informação.